(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2002 (10.01.2002)

PCT

(10) International Publication Number
WO 02/03214 A1

(51) International Patent Classification[7]: G06F 15/00, H04Q 7/38

(21) International Application Number: PCT/CN00/00364

(22) International Filing Date: 27 October 2000 (27.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/216,261	6 July 2000 (06.07.2000)	US
60/223,466	7 August 2000 (07.08.2000)	US
09/675,315	29 September 2000 (29.09.2000)	US

(71) Applicant *(for all designated States except US)*: **CHEUNG KONG (HOLDINGS) LIMITED** [CN/CN]; Cheung Kong Centre, 7th floor, 2 Queen's Road Central, Hong Kong (CN).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **TSUI, Chikong** [GB/CN]; 27 B Yukon Court, 2 Conduit Road, Hong Kong (CN).

(74) Agent: **CHINA PATENT AGENT (H.K.) LTD.**; Great Eagle Centre, 22/F, 23 Harbour Road, Wanchai, Hong Kong (CN).

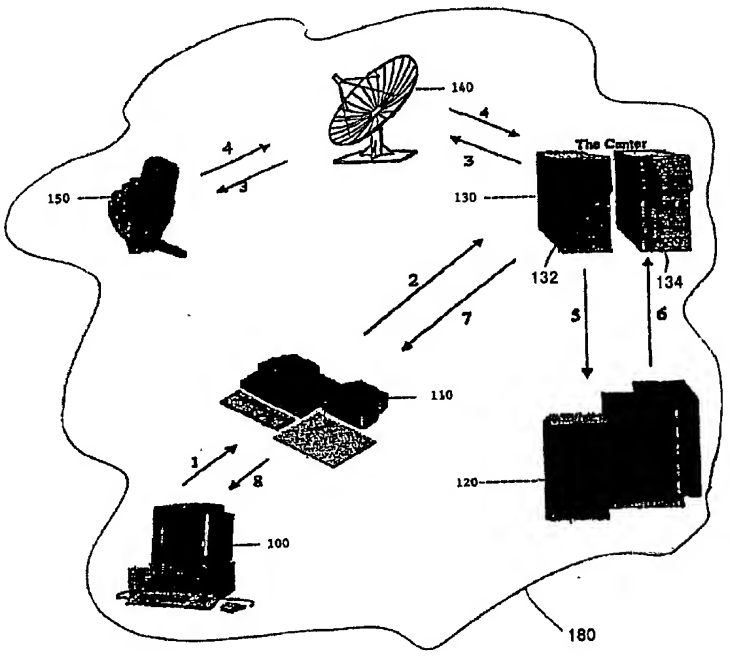
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: CERTIFICATION SYSTEM



(57) Abstract: A method, system, and apparatus for implementing a technique for approving a transaction in a secure manner in an electronically connected network.

WO 02/03214 A1

CERTIFICATION SYSTEM

BACKGROUND OF THE INVENTION

This invention relates to a method, system, and apparatus for providing security, confidentiality, and authenticity for networked transactions.

Currently, several encryption/decryption standards for e-commerce exist to give legal binding effect to transactions. For example, the Public Key Infrastructure (PKI) uses public keys for encryption and digital signatures to provide for confidentiality of information, authentication of actors, integrity of data, non-repudiation of actions, and access control. One example is the PKI service platforms deployed by VeriSign of Mountain View, California. Detailed information about PKI architecture by VeriSign and other vendors can be found in *The VeriSign World Trust PKI Architecutre*, VeriSign White Paper #98-05, 1998, and in *VeriSign Public-Key Infrastructure—Enterprise Key Management*, VeriSign White Paper #98-02, 1998, both of which are incorporated herein by reference. Other encryption/decryption standards include the Data Encryption Standard (DES) and the Secure Sockets Layer (SSL). The features of encryption/decryption standards establish the environment of confidence and trust required for electronic business transactions. However, there are additional Internet transaction security problems that need to be considered. The followings are some examples of the drawbacks of the current system.

Firstly, there are difficulties for the Certificate Authority (CA) to perform real time certificate verification. Most CAs can only recognize whether the certificate is valid, but there is a lapsed time to update the revocation list.

Secondly, when a holder loses his/her authentication information, for example a password or a private key, it is difficult for the certification authority to accept loss report by telephone calls. Therefore, the holder must appear in

person at the CA to ensure that report of loss is genuine. The problem can become worse if there is a long holiday.

Thirdly, if the holder is out of town, it becomes extremely difficult to report a loss. Prior to reporting, an imposter may impersonate the holder of the authentication information online.

Fourthly, because of the above, it is very dangerous to use digital signature to conduct transactions involving large amounts of money. Therefore, most CAs will only accept liability up to a predetermined amount.

Lastly, it is inconvenient for most of the users to implement encryption/decryption standards into their personal computer.

Therefore, there is a need for a certification system to solve the above mentioned drawbacks.

SUMMARY

The present invention is a confirmation system that covers purchases, transactions, or any business interactions, whether over the Internet, through the use of computer, PDA, phone (be it Wireless Application Protocol –(WAP), mobile or wired phone) or in a face-to-face situation.

Regardless of how, where, or when the sale is conducted, the sale can be directly confirmed by the purchaser through means such as a fixed-line phone, mobile or WAP phone, PDA, pager, or any wireless application means or computer by sending a voice message, data message, key punching, PIN or password, whether using PKI, fingerprint authorization, eyeball recognition technology or voice recognition technology, to a process center. The process center may store the purchaser's information including the purchaser's personal information, communication network address or telephone number of the purchaser for confirmation use. The confirmation may also be sent to the merchant directly, thus providing identification, authorization as well as an alerting function to the merchant and customer.

The present invention can be combined with a payment gateway in the back end of the entire process, greatly tighten the security regarding payment in an e-commerce situation. The present invention is applicable to B2B, B2C, C2C or Government to Business or Consumer (G2B or G2C) e-commerce transaction

In general, in one aspect, the Certification System ("CS") is the system designed to use wireless internet technology to improve security in internet transactions. The CS authenticates the registered users in an e-commerce or regular transaction using a wireless internet protocol. For example, the Wireless Application Protocol (WAP) is an open, global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly. An overview discussion of the WAP technology can be found in *Unwiring the Web: Building Dynamic WAP application with ColdFusion* by Azhar, the entire disclosure of which is herein incorporated by reference. A user of the CS can confirm Internet transactions with legal binding effect.

In another aspect, this invention is about the method and system of confirming a transaction, whether face-to-face or electronic, by checking user identification information against user authentication information. User identification can be sent from a user to a processing center. This can be sent directly or through a third party. The processing center looks up other commercial information associated with the user identification information, and generats a confirmation message. The user confirms the transaction by sending user authentication information in response to the confirmation message. In one implementation of the invention, this confirmation message comprises a dynamically generated mobile key including a randomly generated number or an alphanumeric string. The user sends back authentication information by affirming the receipt of the confirmation through the phone or through a terminal. This terminal can be the same as the terminal through which the user

identification information is sent, or it can be a different terminal. In another implementation of the system, the confirmation message comprises an encrypted message using a public key. The authentication information from the user would be a decrypted message by the use of the private key of the public key-private key pair. The generation, management, and maintenance of the public key-private key pair can be done by software provided by a number of providers, such as the RSA BSAFE by RSA Laboratories of Bedford, Massachusetts, or the Hongkong Post e-Cert Certificate by the Hong Kong Post. Detailed information about such software products is available in PKCS #1 v2.1: *RSA Cryptography standard*, or in the *Explanatory Notes* accompanying the application for Hongkong Post e-Cert Certificate, both documents are incorporated herein by reference.

In another aspect, the invention is about the method and apparatus associated with a processing center which hosts commercial information associated with registered users. Upon receiving identification information associated with registered users, the processing center generates a confirmation message to be sent to the user at a stored communication network address. Upon receiving the confirmation message, the user sends back information authenticating that s/he indeed initiated a transaction. The processing center then verifies that the user authentication information matches the user identification information, and issues an approval for the transaction.

Details of one or more embodiments of the invention are set forth in the accompanying drawings and the explanatory description provided below. These embodiments are for illustrative purposes only and the principles of the invention can be implemented in other embodiments. Other features and advantages of the invention will become apparent from the following description and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is an overview diagram of an on-line shopping payment confirmation system implemented in accordance with the principles of the invention.

FIG. 2 is a flow chart illustrating the execution steps of the implementation illustrated in FIG. 1.

FIG. 3A is an exemplary database for customer-related information stored in a processing center; FIG. 3B is an exemplary database for merchant-related information stored in the processing center; FIG. 3C is an exemplary database for transaction-related information stored at the processing center; FIG. 3D is an exemplary database for actions taken within a transaction.

FIG. 4 illustrates a credit card payment scheme implemented in accordance with the principles of the invention.

FIG. 5 illustrates an invoice presentment and settlement scheme implemented in accordance with the principles of the invention.

FIG. 6 illustrates an Internet purchase scheme using the dynamic authentication system implemented in accordance with the principles of the invention.

FIG. 7 illustrates a transfer of fund between accounts using the dynamic authentication system implemented in accordance with the principles of the invention.

FIG. 8 is a screen shot of an exemplary user terminal serving as an entry point for a virtual shopping mall implementing the features of the invention.

FIG. 9 is a screen shot of an exemplary user confirmation terminal for receiving confirmation messages from the processing center in accordance with the principles of the invention.

Like parts in different figures are identified by like numbers.

DETAILED DESCRIPTION

According to the principles of the invention and in one implementation, the CS comprises a center (also called a processing center) responsible for handling certificate issuance, revocation and verification. In one implementation of the system, the certificate comprises two parts -- user identification information and user authentication information.

The user identification information comprises information that identifies the user and can include, for example, a userid, a public key, and user's name.

The user authentication information comprises information used to verify that the transacting party is the user identified by the user identification information, as opposed to an imposter. The user authentication information can comprise, for example, a password, a message decrypted by a private key, or mother's maiden name.

Referring to FIG. 1, the user's authentication tools such as the private key is stored, in one implementation, into the user's confirmation terminal 150. The terminal 150 can comprise any electronic data input/output interface such as a computer system, notebook, notepad, electronic organizer, palm top, cellular phone, pager, or personal digital assistant. The private key in one implementation is the private key of a public key-private key pair issued by certificate authority according to X.509 specification. The public key is stored at the center 130, and the private key is stored at confirmation terminal 150. In one implementation of the invention, if the user already has a key certificated and his/her own public/private key pair, the center 130 will simply register and store the information. If the user does not have a key pair, the center can also issue one. The private key can be loaded into confirmation terminal 150 by proprietary software, such as that supplied by the Hong Kong Post for example, if confirmation terminal 150 is a personal computer. If the confirmation terminal 150 is a WAP phone, the private key can be loaded unto to the phone by

wireless application tools such as the enhanced SIM card platform GemXplore Trust by Gemplus of Cedex, France, or other similar smart card-based applications. Methodology for developing smart card-based applications is explained in *Developing Smart Card-Based Applications Using Java Card* by Jean-Jacques Vandewalle and Eric Vetillard, the entire disclosure of which is incorporated herein by reference. Private keys can also be password-protected at confirmation terminal 150 for additional security.

The user's terminal 100 is either associated with or can access data sent to a communication network address. In one implementation of the system, the user terminal 100 is used to send user identification information. A communication network address comprises an address in a communication network system, or transaction system, 180. Within communication network system 180 information is passed back and forth between terminals and centers and other nodes through the use of the Internet (or other similar global networks), public switched telephone network, or public land mobile network. Within network system 180 data can be sent to and accessed by the user. A communication network address can include, for example, a phone number, email address, or an Internet Protocol address.

In one implementation, the user's terminal 100 is a public terminal accessible to more than just the user. In another implementation, the user's terminal is the same as confirmation terminal 150. In one implementation, all user authentication activities should go through the user's terminal 100 for security purposes. The user authentication information may be protected by an additional password to prevent an imposter with access to the user's terminal 100 from using the authentication information. If the user loses the user's terminal 100, the user should report to the Center 130 immediately. Following the report, the communication network address and user authentication information can be terminated, thereby preventing an imposter from impersonating the user.

In addition to the user's identification data, all personal data such as the user's credit card number, user's name, communication network address or bank accounts are stored in the data base server located at the Center 130. Users only need the user id or the customer id, to transact.

In one implementation of the invention, verbal confirmation can be achieved within system 180 wherein the user terminal 100 is configured to receive voice input from the user. In this case, the user can answer the confirmation with his/her voice through user terminal 100. The voice clip together with authentication information will be sent to the Center 130 to do the matching.

All transaction records are stored in servers 132 and 134 at the Center 130. An exemplary transaction record 370 is illustrated in FIG. 3C. Transaction 370 comprises, among others, customer id 302, merchant code 354, date 374, time 376, transaction amount 372, , and transaction number 382. The items included in record 370 can vary for the various implementations of the invention without deviating from the spirit of the invention. In particular, date 374 refers to the date of the transaction, time 376 refers to the time of the transaction, transaction amount 372 represents amount of the transaction. In one implementation, the maximum amount allowed per transaction is predetermined and cannot be exceeded. Each transaction number 382 may be associated with one more actions items listed in activities log 330 of FIG. 3D. For example, the center can define action code as follows:

1 for place order

2 for confirmation of purchase by customer

3 for cancel a transaction

4 for ask for payment approval

5 for grant payment approval

6 for seek the approval from the bank

7 for grant approval by the bank

8 for ask for order/payment confirmation

9 for confirm the transaction by the center

Supposing that a customer with a value of 100001 for customer id 302100001 makes a purchase from his terminal 100 at 10:30 a.m. on 6/9/2000. This message was received by the Center 130 immediately through the merchant named DEMO 110. The center 130 then sends a message to the customer's device 150. The customer could give confirmation to the center at 11:00. Then, the center 130 asked the payment approval from the bank. Finally, the center would give final confirmation to the merchant to finish the transaction. In this case, the following records are written on the database under activities-log 330 as:

Date (332)= 20000906

Time (334) = 1030

Action-code (336) = 1

Action-details (338) = 100001 place order to merchant DEMO

Transaction-number (382)= 1234567

Merchant-code (354)= DEMO

Date (332)= 20000906

Time (334)= 1040

Action-code (336)= 4

Action-details (338)= DEMO ask for payment confirmation

Transaction-number (382) = 1234567

Merchant-code (354)= DEMO

Date (332) = 20000906

Time (334)= 1041

Action-code (336) = 8

Action-details (338)= The center ask 100001 for payment confirmation

Transaction-number (382) = 1234567

Merchant-code (354)= DEMO

Date(332) = 20000906

Time (334)= 1100

Action-code (336)= 2

Action-details (338)= 100001 confirmed the purchase

Transaction-number (382)= 1234567

Merchant-code (354)= DEMO

Date (332) = 20000906

Time (334) = 1101

Action-code (336)= 8

Action-details (338)= The center ask the bank for payment approval

Transaction-number (382)= 1234567

Merchant-code (354) = DEMO

Date (332)= 20000906

Time (334)= 1102

Action-code (336)= 5

Action-details (338)= The bank granted the payment approval
Transaction-number (382) = 1234567
Merchant-code (354) = DEMO

Date (332) = 20000906
Time (334) = 1102
Action-code (336) = 9
Action-details (338) = The center confirm the transaction to DEMO
Transaction-number (382) = 1234567
Merchant-code (354)= DEMO

All above actions should be associated with transaction 1234567 as an entry in transaction record 370 as:

customer-id (302) = 100001
transaction-number (382) = 1234567
merchant-code (354) = DEMO
tx-amount (372)= 1567
tx-date (374) = 20000906
tx-time (376) = 1102

In one implementation, there will be no record written in transaction record 370 if the transaction has not been completed. Transaction number 382 refers to a unique transaction number associated with each transaction and is used to cross-reference record 370 and log 330. In one implementation, all transactions will have legal binding effect on all the involved parties; the Center 130 will be

authorized to provide online services to computer users and merchants who need online transaction confirmation for legal purposes.

Numerous implementations of the invention are possible. A network provider can provide infrastructure for communication purpose to multiple parties. For example, bankers can join as registered users to provide online banking services. Credit card companies can use this system to communicate with cardholders to confirm transactions, thus alleviating the risk of fraudulent transactions caused by lost cards. In a Business-to-Customer or Business-to-Business situation, the center 130 can provide regular statements to the customers and the merchants in respect of the completed transactions using the CS. This will ease the administrative workload of the merchants and provide checking services to the customers and merchants to help merchants/customers detect early any abuse by their employees/friends who are in charge/have the merchants/customers' authentication information. These various implementations of the principles of the invention will be illustrated in the other drawings.

FIG. 1 is an overview diagram of an on-line shopping payment confirmation system ("OLSPCS") 180, a system implemented in accordance with the principles of this invention. Under the OLSPCS 180, a customer may make a purchase via public network with the following steps. The user first selects (step 1) merchant 110 and goods via public via a network connection through a user terminal 100. A user terminal comprises a number of electronic communication devices listed above, or it can also comprise a face-to-face interaction. Once the selection is made, the user identification information is submitted (1) to the merchant 110, which then sends (2) the user's identification information, user's name and/or other identification information to the center 130.

The center 130 will check against the database to see if it is a valid user or if the user is in the revocation list. Exemplary customer information for each registered user is illustrated in table 300 in FIG. 3A. Relevant customer information comprises customer ID 302, customer phone number 304, mobile phone number 306, e-mail address 308, bank name 310 listing the customer's preferred transaction bank, bank account number 312, address 316, credit card type 318 listing the preferred credit card specified by the customer, credit card number 320, and status 322 indicating the registered user's status as valid or revoked, and an expiration date 324, reflecting the expiry date for the registration period of the center. Merchant information is also stored at center 130, as illustrated in table 350 in FIG. 3B, including merchant code 354, merchant's account number 356, and the amount limited, such as per transaction, 358. The contents of tables 300, 330, 350, and 370 can be any combination, subset, and/or superset of the various types of information listed above without deviating from the spirit of the invention.

If the user identification information corresponds to a valid user, the center 130 will send (3) a confirmation message to the customer using the communication network address using a communication network, such as via satellite 140, associated therewith to ask if he/she will approve the payment.

The customer receives the confirmation message at a confirmation terminal 150. In one implementation, the confirmation terminal 150 is different from the user terminal 100. In another implementation, the confirmation terminal 150 is the user terminal 100. In yet another implementation, the customer may receive the confirmation at the confirmation terminal 150, but authenticates him/herself at the user terminal 100. Of course the customer can also receive confirmation and returns authentication at confirmation terminal 150 in other implementations of the invention.

The customer chooses either approval or rejection verbally or otherwise

through the user terminal 150. The reply is then returned (4) to the Center 130 through the same or different network. In one implementation, the confirmation terminal 150 is a wireless WAP; in other embodiments the confirmation terminal 150 comprises a regular cell phone, a pager, a computer, a fixed line phone, or a number of other possible electronic devices. The customer is required to supply their authentication information to ensure their identification. Once the center 130 receives the customer's payment approval, it will check if the user authentication information matches previous user authentication information. In one implementation of the invention, each user should have an unique mobile key issued by the center, comprising, for example, a randomly generated number or an alphanumeric string. A unique key will be generated by the center for each transaction. The customer will use this key to confirm the transaction with a transaction number by calling or otherwise communicating the information back to center 130, such as by entering and sending the randomly generated number constituting the unique key through user terminal 100. After verification, the center 130 will send (5) a request for payment approval with the customer credit card information to the bank hub 120.

The bank hub 120 will grant (6) approval for payment to the merchant 110 through Center 130. Center 130 confirms (7) payment with merchant 110, which arranges (8) for goods delivery to the user. In one implementation, merchant 110 instructs the center 130 to issue a digital receipt and to send the digital receipt to the user using the communication network address.

FIG. 2 is a flow chart of operation steps involved in transaction system 180. Although not shown here in the flow chart, as a preliminary step, registration of users should be conducted. User id and other commercial user information should be loaded and stored at Center 130 before a transaction starts. The users start by providing their user identification information (box 20). The bank or bank hub 120 or merchant 110 receives the user identification

information and forwards it to the center 130, also known as the Service Provider (SP) or processing center (box 22). The center 130 then receives the user identification information and performs the validation process according to information stored in the database (box 24). If the user identification information does not correspond to a valid user (box 26), it is rejected and the database is updated (box 36). If the user identification information corresponds to a valid user, a confirmation message is sent to the confirmation terminal 150 using the communication network address (box 28). The user will then access the confirmation message using confirmation terminal 150, which may be identical to user terminal 100 in some implementations, and reply using the user authentication information (box 30). In one implementation, each customer should have a private key to do the authentication. In another implementation, the customer can do the authentication by a dynamic key which is generated by the center 130. Optionally, a table call "customer-policy" may be added to specify authentication policies for each customer. The detailed items are as follows:

Customer-id
Action-code
From-tx-amt
To-tx-amt
Effective-date
Termination-date

With this table, a customer can define a set of rules for the center to execute verification accordingly.

If the user authentication information does not match the user identification information (box 32), the transaction is rejected and the database is updated (box

36). Else, the center 130 checks to see if the user approved the payment. If yes, a confirmation is sent to the bank 120 or merchant 110 (box 38). Else, it is rejected (box 34) and the database is updated (box 36). In one implementation, the database is updated periodically at every checkpoint.

Exemplary and specialized implementations of transaction system 180 for certain specific uses are illustrated below:

Credit Card Payment Confirmation

Referring to FIG. 4, in the case of a normal credit card payment, the credit card holder can also use this service. The center 130 will have a pre-arrangement with credit card companies which is in connection with credit card center 410. Once a merchant swipes the credit card to ask for payment authorization in a face-to-face, telephone transaction, or other types of electronic transaction situation 400, the credit card number will be sent (42) to the credit card center 410. For those credit card companies facilitating this service, they can send the user identification information to the center 130 to ask (44) for payment approval. Center 130 uses the user identification information to retrieve the communication network address and then send (45) dynamic confirmation information comprising a dynamic key, encrypted message, or the like In this case, the center will check with the customer-policy table to determine which action should be taken. If the customer defines that only those transactions exceeding HK$10,000 should obtain approval before processing. If the current transaction amount is less than HK$10,000, the center may only issue acknowledgement to the customer. Otherwise, a dynamic key with transaction number will be issued to the customer for payment approval purpose to the customer's confirmation terminal 150 over a communication network using the user's communication network. The user can confirm (46) payment over the same communication network by approving or declining payment. If the purchase is confirmed (47) via center 130, a credit card payment receipt will then

be issued (48) for signing by the customer in location 400. If the center receives a negative signal or if no signal is received by center 130 within a predetermined period of time, for example 10 minutes, no credit card payment receipt will be issued by the credit card center (410). The foregoing illustrates an advantage of one embodiment of the invention enabling the customer to be alerted in real-time that their credit card is being used. The risk of lost cards is thereby reduced.

In other embodiments of the invention, the customer can confirm the payment by the user terminal 100 or other terminal. If the customer gives confirmation by phone 150, the center 130 will have a system to answer the call automatically and stores all reply information such as transaction number and the dynamic authentication information to the database, such as in activities log 330.

In yet another embodiment of the invention, center 130 can also implement different levels of authorization as per the request of each user or customer. For example, a user can specify that a simple notification or confirmation message is enough for those transactions below US$100. If the transaction amount is greater than US$10,000, the user may desire the highest secured authorization procedures. For example, the center will request the user to provide a digital signature using a private key to confirm the transaction.

Bill Presentment & Settlement

Customers and merchants can settle all bills through this system. First of all, customers must register each bill's information such as merchant code, account number and settlement bank account number into the system. Referring to FIG. 5, those merchants who are members of center 130 can send (50) billing information 500 comprising monthly bills to the center 130 through the Internet instead of by postal service. The center 130 then will inform (52) customers at confirmation terminal 150 that the bills have been received and the total amount is indicated through the mobile operator or the pager operator or

any communication network operator as specified by the customers. A dynamic authentication information with bill transaction number is also sent to the user's communication network address. If the user wants to see the details of a bill, they can get detailed information through the Internet. At the same time, he/she can settle the bill by replying (3) to the center 130 with the corresponding dynamic authentication information by confirmation through the user terminal 100 or confirmation terminal 150 comprising customer's mobile phone, PC or any communication network or the like. Once the confirmation is received by the center 130, the center 130 will instruct (54) the client's bank 120 to settle the bill accordingly. Settled bills will be returned (55) to merchants.

Dynamic Authentication Information

It is noted that PKI is user-unfriendly and can still be stolen by others. Therefore, in another implementation, the use of dynamic authentication information to confirm the transaction is used.

Referring to FIG. 6, when a customer registered with center 130 wants to make a purchase whether through the Internet or in face-to-face situations, s/he is only required to supply (61) a user identification information to the merchant 110. The merchant 110 then will send (62) this user identification information to the center 130. Based on this user identification information, the center 130 can retrieve all information about the customer such as banking information and communication network address, such as those listed in table 300. Center 130 can also check (65) with credit card center 410 and receive (66) approval. The center 130 will generate a unique key for confirmation purposes. Center 130 forwards (63) such information to the customer using the communication network address. The dynamic authentication information comprises, for example, a key or password. When the customer receives the dynamic authentication information through the communication network address at

confirmation terminal 150, which may comprise a mobile phone, WAP phone, fixed-line phone, pager or other similar devices, s/he uses user terminal 100 or any terminal to confirm (64) the purchase and payment over a communication network. The center will check against the database. If the dynamic authentication information received from confirmation terminal 150 is matching, the payment will be confirmed (67) with merchant 110 to deliver (68) purchased goods. Because the dynamic authentication information will be generated for every transaction, it is protection against being stolen and provides an extra level of security to electronic transactions.

Other possible implementations of the invention include, but not limited to, the following:

Banking Instruction Confirmation

Referring to FIG. 7, when a user wants to do fund transfer from his bank A account (785) to an account of another bank (775) through cyber banking, the user can supply (71) the user identification information to bank A 785 through the Internet banking program. The user is not required to input their account number in this case.

The bank A 785 will transmit (75) the user identification information to the center 130 and expect a confirmation from the center 130. Based on the user identification information, the center 130 retrieves the user's communication network address form the database and then sends (73) the request for confirmation to the user using the communication network address over the communications network associated therewith. The user answers (74) the confirmation with the user authentication information.

The center 130 will check the user authentication information with the previous user identification information and/or confirmation to see if they match. An approval will be sent (72) to the bank A 785 via the communication network after certificate validation. The bank A then takes action (76) with respect to

bank B 775 accordingly with the confirmation from the user. Other than funds transfer amongst different banks, this application will facilitate the customer to buy shares through his brokers without first manually depositing monies to his broker's account but just transferring the monies electronically. This approach offers the advantage of conducting sale and purchase of shares through a number of brokers rather than restricting the customer to one broker for provision of securities services.

Order Confirmation

Yet another implementation of this invention entails the following. It is not uncommon that the merchant will give credit to its old customers. Meanwhile, there should be some form of confirmation from customers to acknowledge the issuance of order via online shopping system.

When the customer takes order through online system, he will be required to confirm the purchase order with digital signature. Therefore, he/she needs to supply his/her user identification information to the merchant firstly.

The merchant transmits order information with user identification information to the processing center via public network. The processing center will perform validation procedures and then transmit information via a communications network to the customer's communication network address and ask for confirmation.

The customer then checks the order information from his/her user terminal and then issues a confirmation with user authentication information to the processing center. The processing center will give the merchant the purchase confirmation. This confirmation should have legal binding effect on both parties.

When the merchant arranges for delivery, an instruction will be given to the processing center to issue a credit note to the purchase.

In general, in summary, the merchant receives an order from a customer via the communications network operator (which stores the personal information of the purchaser and acts as process center) the transaction information to seek confirmation from the purchaser. The communications network operator sends a message with the generated key, for confirmation purpose, to the customer's designated terminal (for example, mobile phone). The purchaser upon receiving the message from its designated terminal may then use any kind of device to confirm the transaction with the merchant. This validation procedure can prevent any unauthorized purchase made by a person other than the purchaser.

FIG. 8 illustrates a virtual shopping mall as it appears on a screen of user terminal 100. In one implementation, the items offered for sale comprise mobile phones 700, 710, 720, and 730. The user may select the product s/he wishes to purchase by entering the product in dialog box 740, using a pull-down menu or keyboard input or ther input means. The user needs to provide userid or Login ID in box 760, and provide e-mail address in 750. The user then clicks button 770 to proceed with the transaction. The items already in the electronic shopping cart can be viewed by clicking button 780.

FIG. 9 illustrates a sample confirmation message 800 as it appears on confirmation 150. With different types of authentication methods, different types of confirmation messages will be generated. For example, if the authenticating tool is a private key of a public-private key pair supported by standard PKI, the confirmation message will be a message encrypted by the public key, which message the user will use the corresponding private key to decrypt, and the decrypted message will be returned as authentication information. The confirmation terminal 150 is shown as a wireless phone in this implementation, but may be other types of electronic interactive devices in

other implementations.

The above system and its associated programs may be associated in a computer-readable medium or any article of manufacture that contains data that can be read by a computer or a carrier wave signal carrying data that can be read by a computer. For example, this invention may be distributed on magnetic media, such as a floppy disk, flexible disk, hard disk, reel-to-reel tape, cartridge tape and cassette tape; optical media such as CD-ROM and the like, and/or paper media such as paper tape; or carrier wave signal received through a network, wired or wireless, or modem, including various types of signals.

The above embodiments of the invention are for illustrative purposes only. Many widely different embodiments of the present invention may be adopted without departing from the spirit and scope of the invention. Those skilled in the art will recognize that the method and structures of the present invention has many applications, and that the present invention is not limited to the specific embodiments described in the specification and should cover conventionally known variations and modifications to the system components described herein.

What is claimed is:

1. A method for approving a transaction over a computer network, said method comprising:

forwarding user identification information to a processing center for an approval of the transaction;

retrieving a communication network address associated with the user identification information;

transmitting a confirmation to the communication network address; and

receiving user authentication information from the communication network address.

2. The method of claim 1, further comprising:

determining if the user authentication information corresponds to the user identification information.

3. The method of claim 2, further comprising:

generating the approval for the transaction at the processing center.

4. The method of claim 2, wherein the transmitting step further comprises:

generating an encrypted message using a public key, stored at the processing center, associated with the user identification information as the confirmation message.

5. The method of claim 2, wherein the transmitting step further comprises:

generating a dynamic mobile key comprising a randomly generated number as the confirmation message.

6. The method of claim 4, wherein the user authentication information comprises a decrypted message using a private key corresponding to the public key constituting a public key-private key pair.

7. The method of claim 5, wherein the user authentication information comprises a verbal affirmation of the randomly generated number delivered through a phone line of a publicly switched telephone network.

8. A computer-readable medium carrying one or more sequences of instructions for confirming a transaction electronically, wherein execution of the one or more sequences of instructions by one or more processors cause the one or more processors to perform the steps of :

forwarding user identification information to a processing center for an approval of the transaction;

retrieving a communication network address associated with the user identification information;

transmitting a confirmation to the communication network address; and

receiving user authentication information from the communication network address.

9. The computer-readable medium of claim 8, wherein the one or more sequences of instructions further comprise instructions to cause the one or more processors to perform the step of

determining if the user authentication information corresponds to the user identification information.

10. The computer-readable medium of claim 9, wherein the one or more

sequences of instructions further comprise instructions to cause the one or more processors to perform the step of:

generating the approval for the transaction at the processing center.

11. The computer-readable medium of claim 9, wherein the transmitting step further comprises:

generating an encrypted message using a public key, stored at the processing center, associated with the user identification information as the confirmation message.

12. The computer-readable medium of claim 9, wherein the transmitting step further comprises:

generating a dynamic mobile key comprising a randomly generated number as the confirmation message.

13. The computer-readable medium of 11, wherein the user authentication information comprises a decrypted message using a private key corresponding to the public key constituting a public key-private key pair.

14. The computer-readable medium of 12, wherein the user authentication information comprises a verbal affirmation of the randomly generated number delivered through a phone lines of a publicly switched telephone network.

15. A method for approving a transaction in a communication network, said method comprising:

forwarding user identification information of a first party from the first party to a second party;

retrieving a communication network address associated with the user identification information at a processing center;

generating a confirmation message at the processing center and forwarding the confirmation message to the communication network address;

in response to the confirmation message, generating dynamic authentication information by the first party;

returning the dynamic authentication information to the processing center;

verifying the dynamic authentication information against the confirmation message; and

generating an approval for the transaction.

16. The method of claim 15, wherein the communication network address comprises an e-mail address.

17. The method of claim 15, wherein the forwarding step is transmitted from a personal computer.

18. The method of claim 15, wherein the forwarding step is transmitted from a personal digital assistant.

19. The method of claim 15, wherein the dynamic authentication information is returned from a WAP (Wireless Application Protocol) phone.

20. The method of claim 15, wherein the dynamic authentication information is returned from a personal computer.

21. A computer-readable medium carrying one or more sequences of

instructions for confirming a transaction electronically, wherein execution of the one or more sequences of instructions by one or more processors cause the one or more processors to perform the steps of :

forwarding user identification information of a first party from the first party to a second party;

retrieving a communication network address associated with the user identification information at a processing center;

generating a confirmation message at the processing center and forwarding the confirmation message to the communication network address;

in response to the confirmation message, generating dynamic authentication information by the first party;

returning the dynamic authentication information to the processing center;

verifying the dynamic authentication information against the confirmation message; and

generating an approval for the transaction.

22. The computer-readable medium of claim 21, wherein the communication network address comprises an e-mail address.

23. The computer-readable medium of claim 21, wherein the forwarding step is transmitted from a personal computer.

24. The computer-readable medium of claim 21, wherein the forwarding step is transmitted from a personal digital assistant.

25. The computer-readable medium of claim 21, wherein the dynamic authentication information is returned from a WAP (Wireless Application

Protocol) phone.

26. The computer-readable medium of claim 21, wherein the dynamic authentication information is returned from a personal computer.

27. An electronically connected system for approving a transaction in a communication network, comprising:

a processing center for receiving user identification information from a first party, said center including a database for retrieving a communication network address associated with the user identification information for receiving a confirmation; and

a first terminal associated with said communication network address for transmitting user authentication data to the processing center in response to receipt of the confirmation at the communication network address.

28. The system of claim 27, wherein the first terminal comprises a WAP phone.

29. The system of claim 27, wherein the first terminal comprises a pager.

30. The system of claim 27, wherein the first terminal comprises a phone wired to a public-switched telephone network.

31. The system of claim 27, wherein the first terminal forwards the user identification information to the processing center.

32. The system of claim 27, further comprising a second terminal for

transmitting the user identification information.

33. The system of claim 32, wherein the second terminal comprises a PC.

34. The system of claim 32, wherein the second terminal comprises a mobile phone.

35. The system of claim 27 or claim 32, wherein the user authentication data comprises a dynamically generated decrypted message.

36. The system of claim 27, wherein the user authentication data comprises a password.

37. The system of claim 27, wherein the processing center matches the user authentication data against the user identification information before issuing an approval for the transaction.

38. The system of claim 35, wherein the confirmation comprises an electronically generated message encrypted by an electronic key.

39. The system of claim 35, wherein the decrypted message is generated using an electronic key stored in the first terminal.

40. The system of claim 35, wherein the decrypted message is generated using an electronic key stored in the second terminal.

41. The system of claim 39 or claim 40, wherein the electronic key is

password-protected.

42. A network-based system for approving a transaction, comprising:

a processing center for receiving user identification information from a seller, said center including a database for retrieving a communication network address associated with the user identification information for receiving a confirmation;

a first terminal associated with said communication network address for transmitting user authentication data to the processing center in response to receipt of the confirmation at the communication network address; and

a second terminal operable by a user for sending user identification information to the seller.

43. The system of claim 42, wherein the user identification comprises a user code comprising an alphanumeric string.

44. The system of claim 43, wherein the user code is associated with commercial user information stored in the database.

45. The system of claim 44, wherein the commercial user information comprises user bank account number.

46. The system of claim 44, wherein the commercial user information comprises user registration status.

47. The system of claim 42, wherein the transaction comprises a face-to-face transaction between the seller and the user.

48. The system of claim 42, wherein the transaction comprises an electronic transaction.

49. An apparatus for securing a transaction electronically, comprising:

a storage device; and

a processor connected to the storage device,

the storage device storing a program for controlling the processor, and

the processor operative with the program to:

receive user identification information;

retrieve a communication network address associated with the user identification information;

transmit a confirmation to the communication network address; and

receive user authentication information from the communication network address.

50. The apparatus of claim 49, in which the processor is further operative with the program to:

transmit a payment authorization upon verifying that the authentication information corresponds to the user identification information.

51. The apparatus of claim 49, wherein the processor is located in a processing center, the processing center hosting a database containing commercial information of registered users.

52. The apparatus of claim 51, wherein the user identification information is transmitted from a WAP phone or a mobile phone.

53. The apparatus of claim 51, wherein the user identification

information is transmitted from a person computer.

54. The apparatus of claim 51, wherein the user authentication information is transmitted from a pager.

55. The apparatus of claim 49, wherein the confirmation comprises a dynamically generated mobile key.

56. The apparatus of claim 51, wherein the confirmation comprises a text message encrypted by a public key associated with a registered user.

57. The apparatus of claim 56, wherein the user authentication information comprises a decrypted message derived from the encrypted text message using a private key corresponding to the public key.

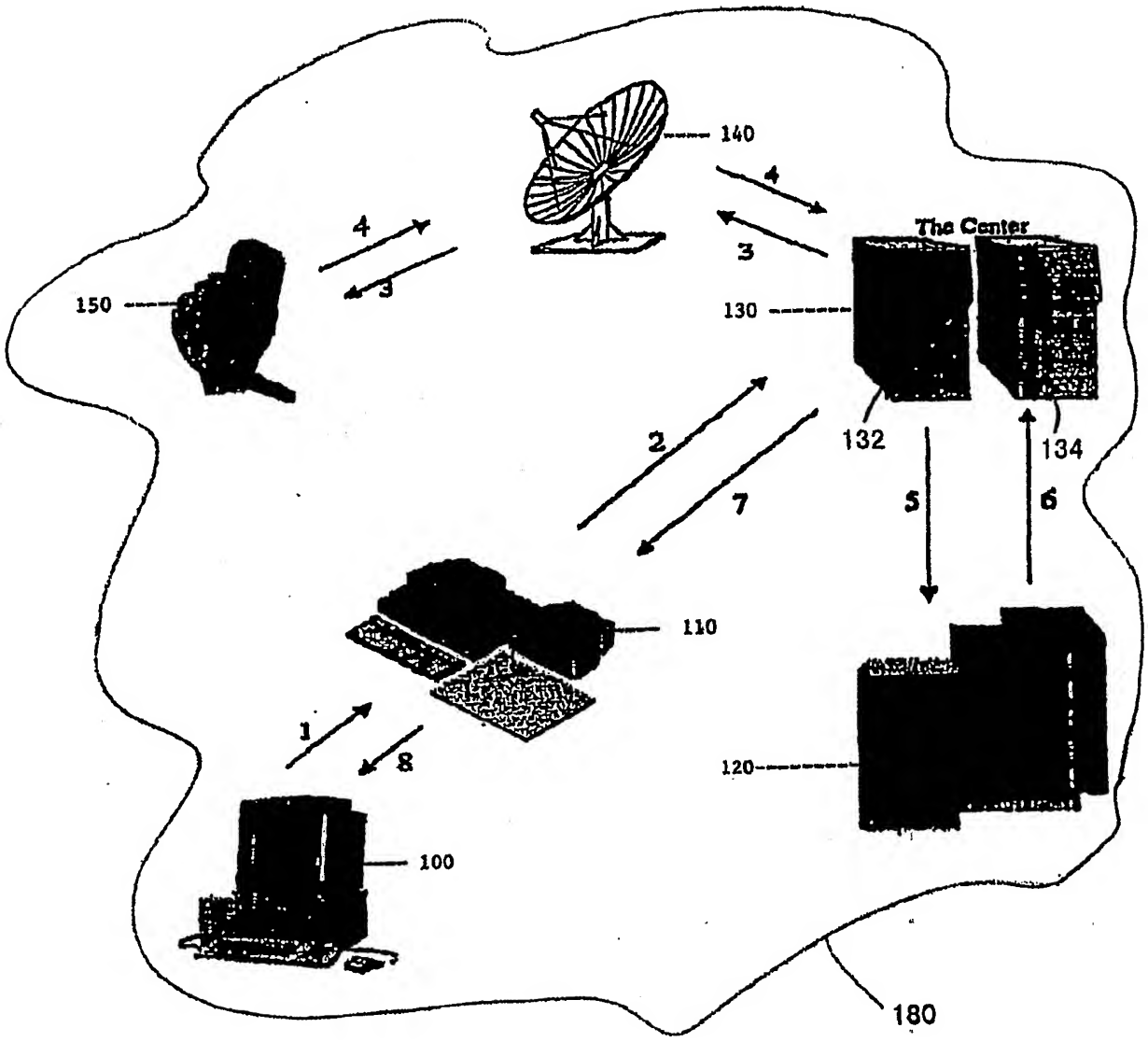


FIG . 1

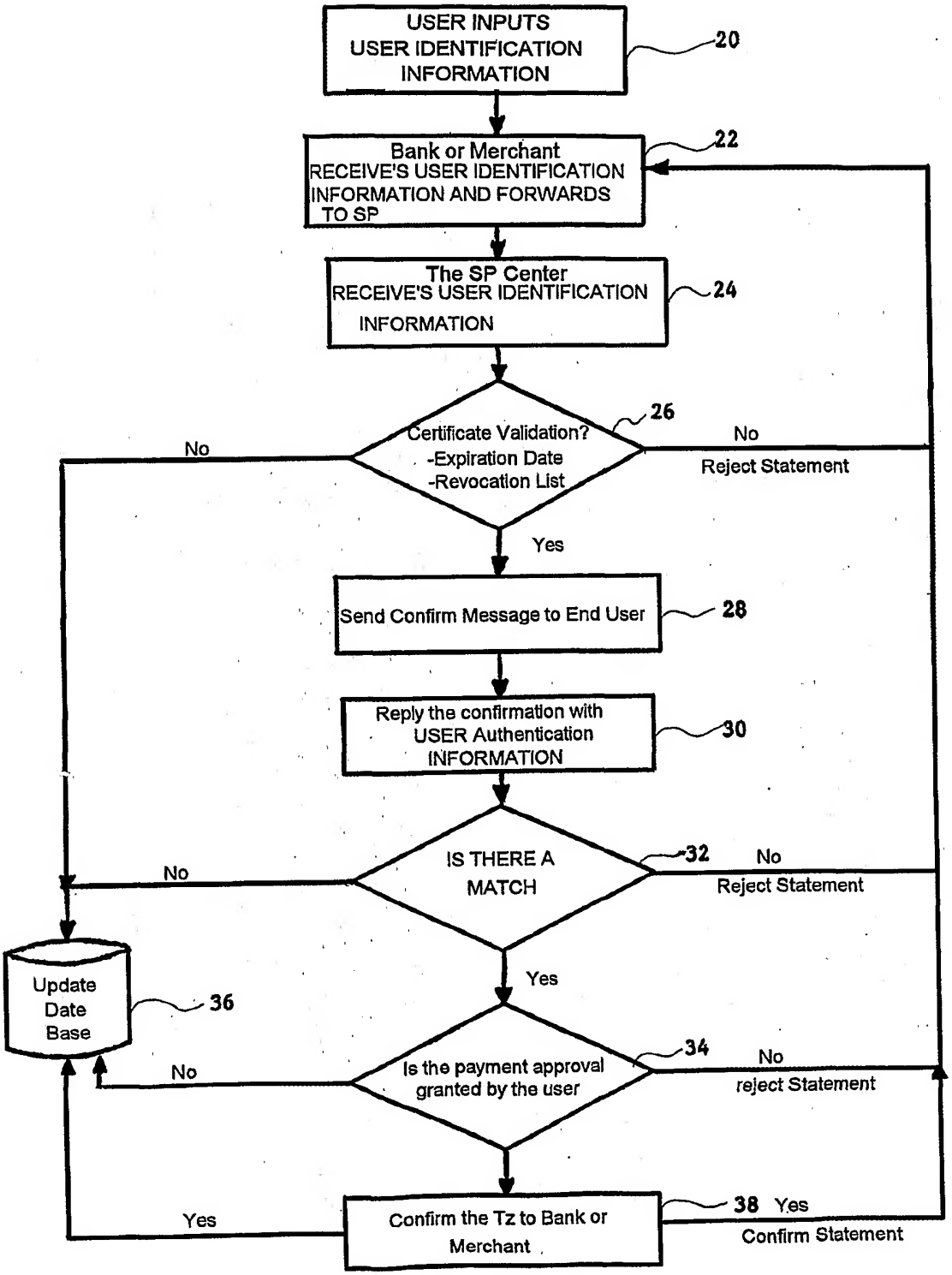

USER INPUTS USER IDENTIFICATION INFORMATION
20
Bank or Merchant RECEIVE'S USER IDENTIFICATION INFORMATION AND FORWARDS TO SP
22
The SP Center RECEIVE'S USER IDENTIFICATION INFORMATION
24
Certificate Validation? -Expiration Date -Revocation List
26
No
Reject Statement
No
Yes
Send Confirm Message to End User
28
Reply the confirmation with USER Authentication INFORMATION
30
IS THERE A MATCH
32
No
Reject Statement
No
Yes
Update Date Base
36
Is the payment approval granted by the user
34
No
reject Statement
No
Yes
Confirm the Tz to Bank or Merchant
38
Yes
Confirm Statement

FIG. 2

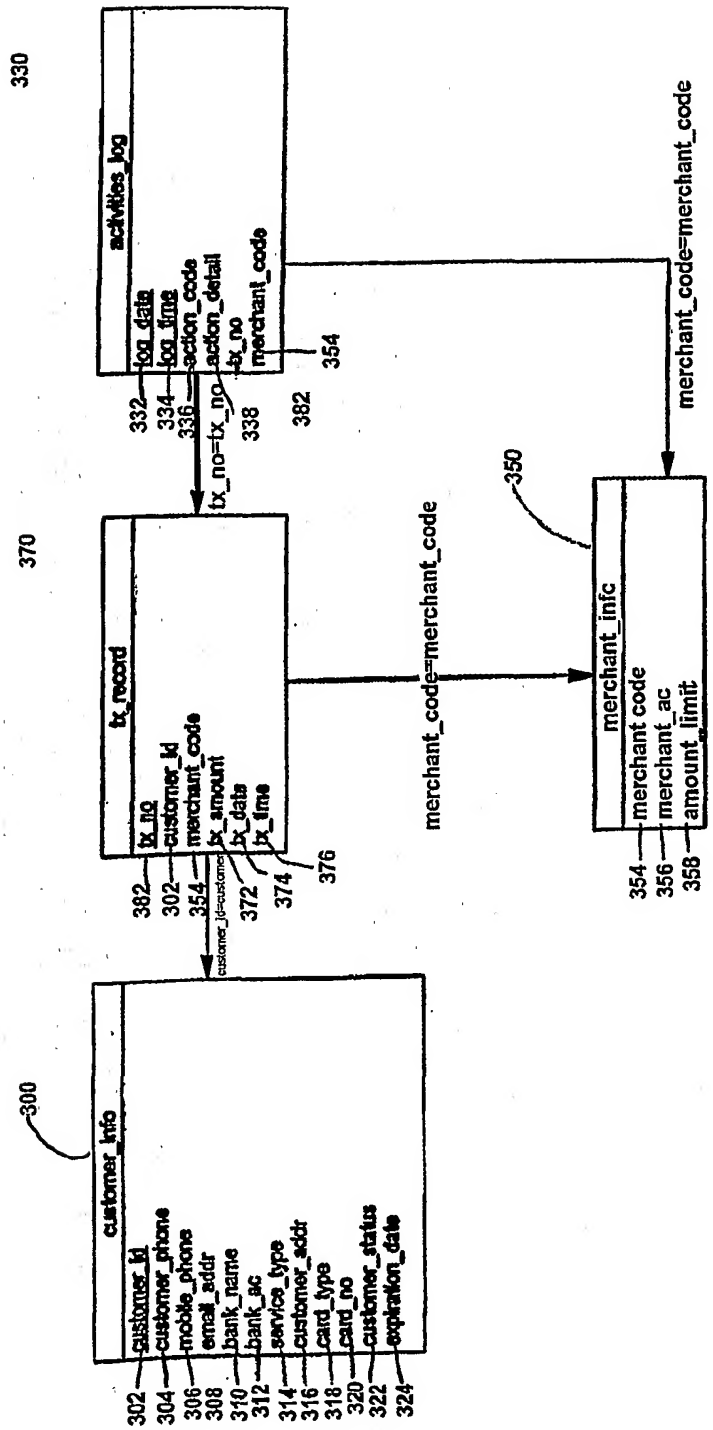

330
activities_log
log_date
log_time
action_code
action_detail
tx_no
merchant_code
332
334
336
338
382
354
tx_no=tx_no
merchant_code=merchant_code
370
tx_record
tx_no
customer_id
merchant_code
tx_amount
tx_date
tx_time
382
302
354
372
374
376
customer_id=customer_id
merchant_code=merchant_code
350
merchant_infc
merchant code
merchant_ac
amount_limit
354
356
358
300
customer_info
customer_id
customer_phone
mobile_phone
email_addr
bank_name
bank_ac
service_type
customer_addr
card_type
card_no
customer_status
expiration_date
302
304
306
308
310
312
314
316
318
320
322
324

FIG. 3

Credit Card Payment Confirmation

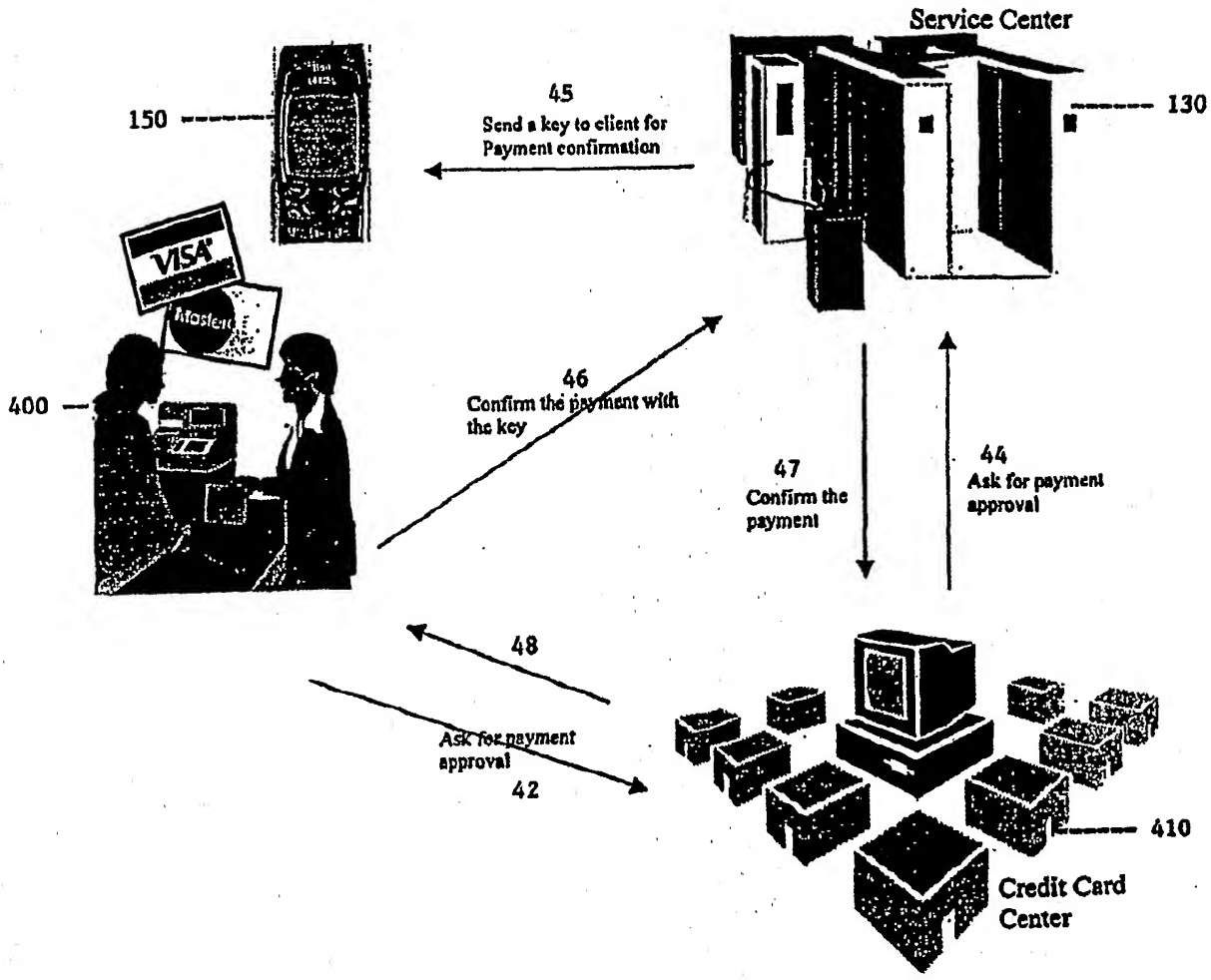


FIG . 4

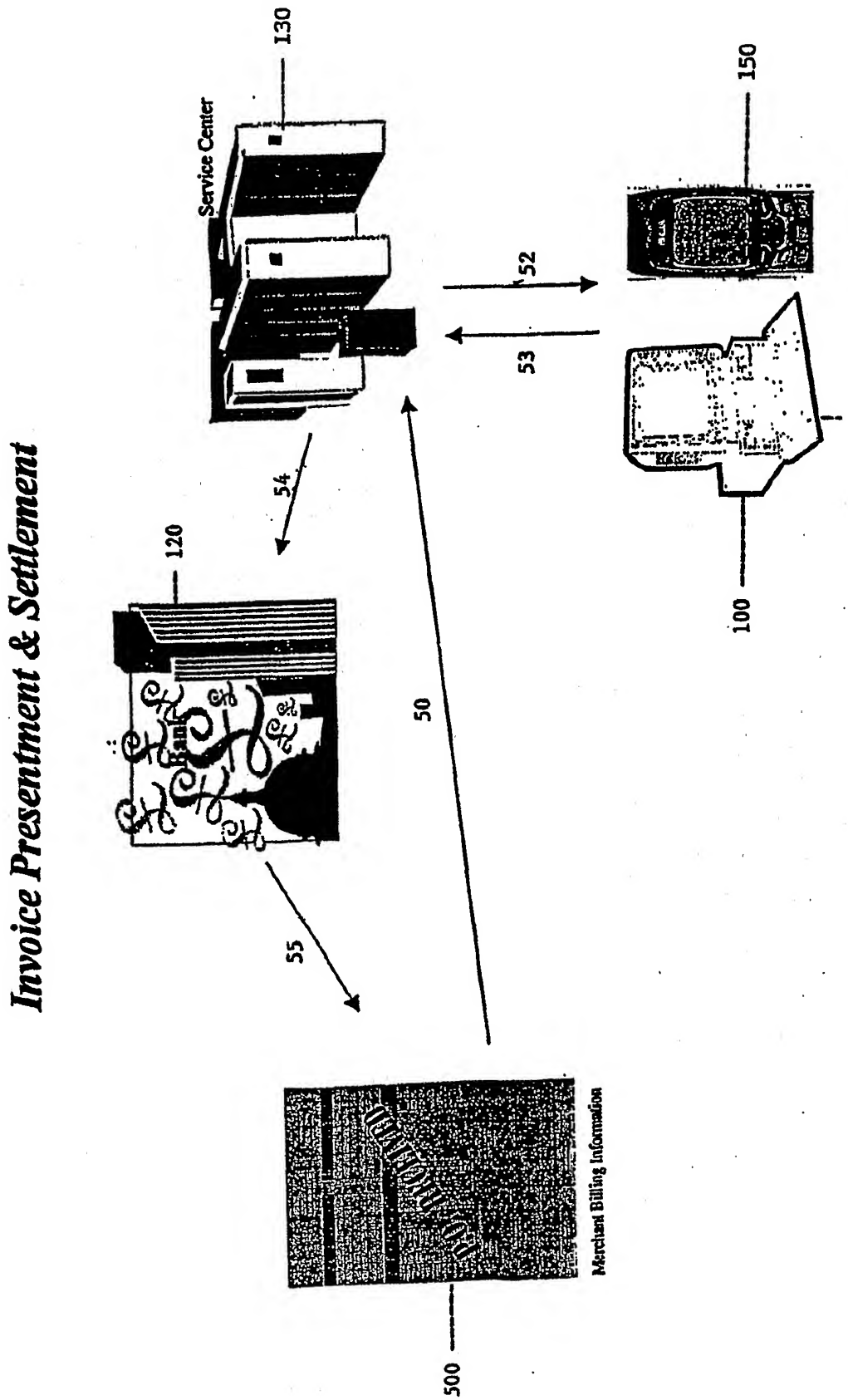

Invoice Presentment & Settlement
130
Service Center
150
52
53
54
120
Bank
50
55
100
500
Merchant Billing Information

FIG. 5

Internet Purchase Through Dynamic Authentication System

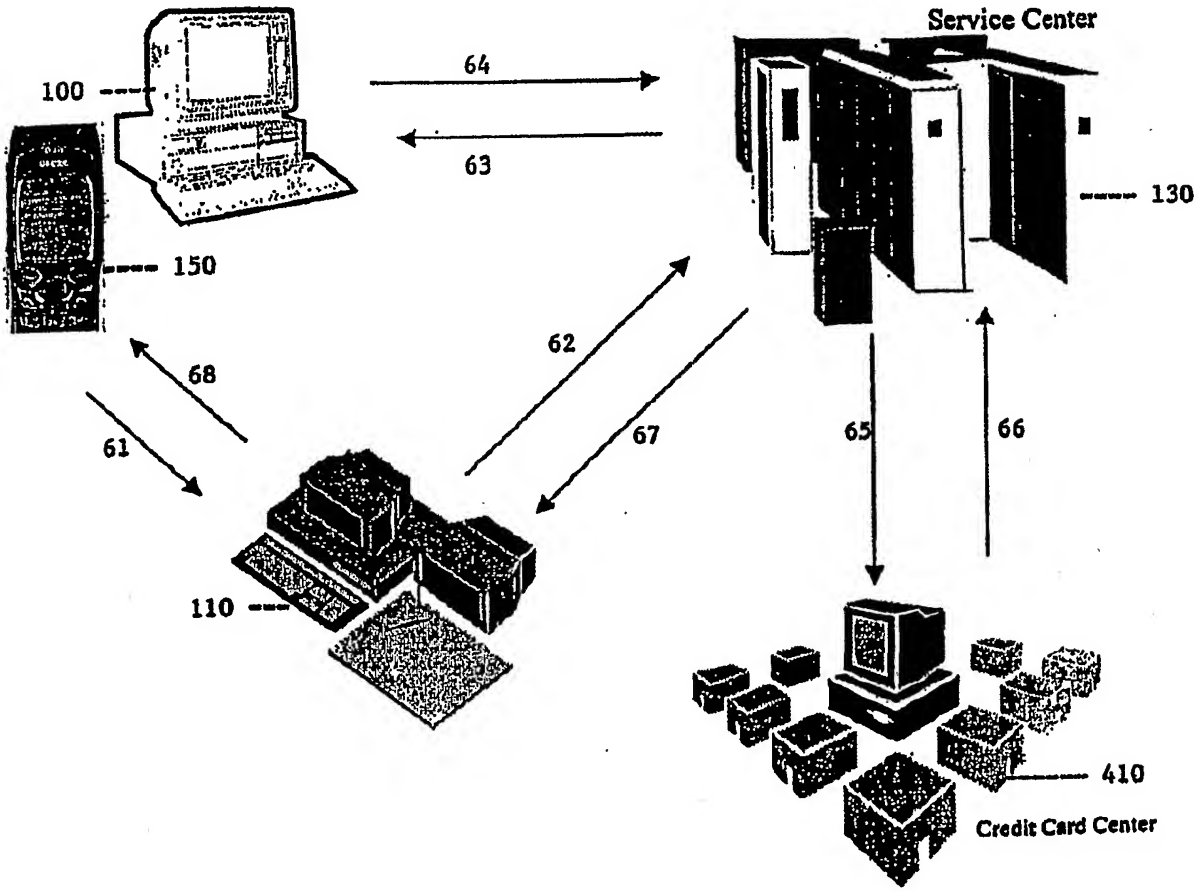


FIG . 6

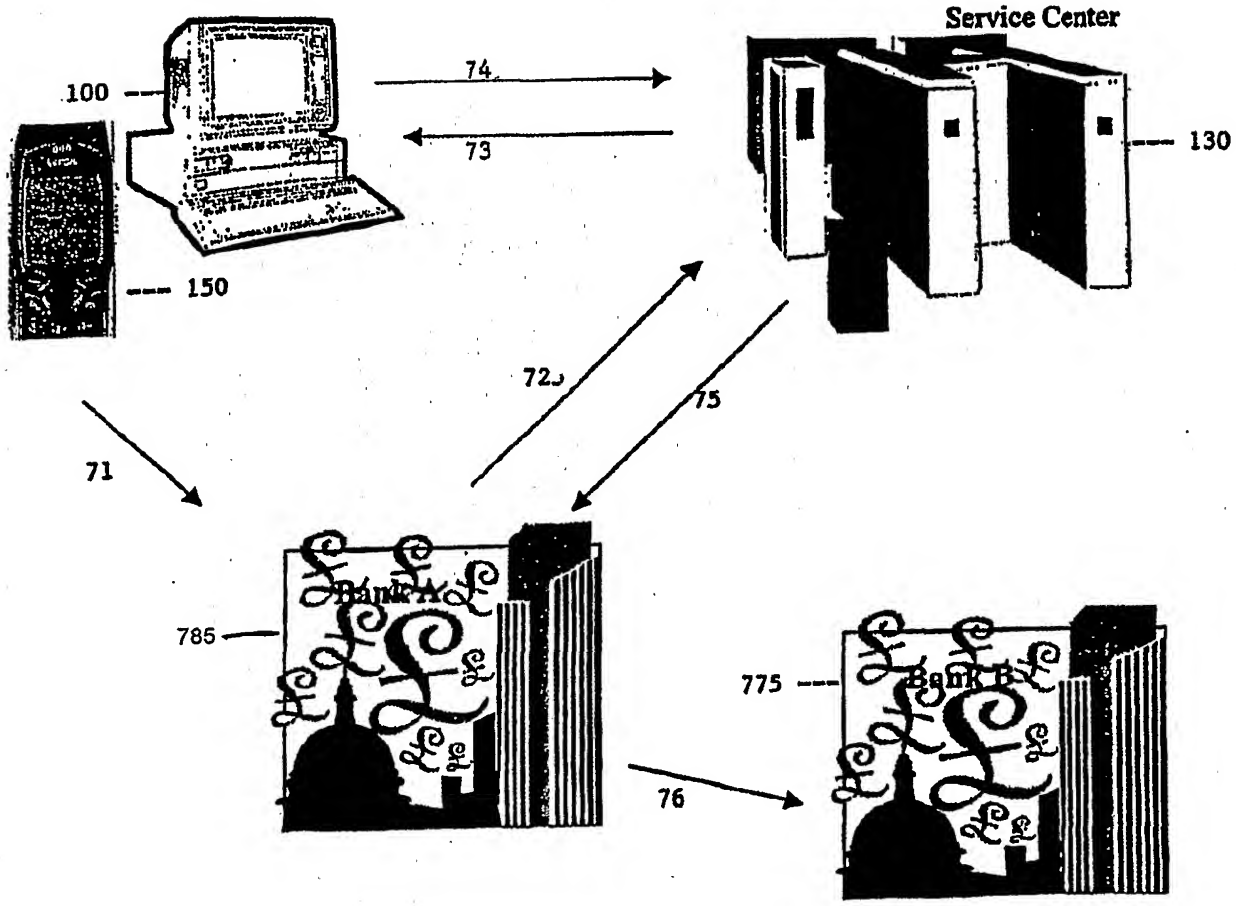


FIG .7

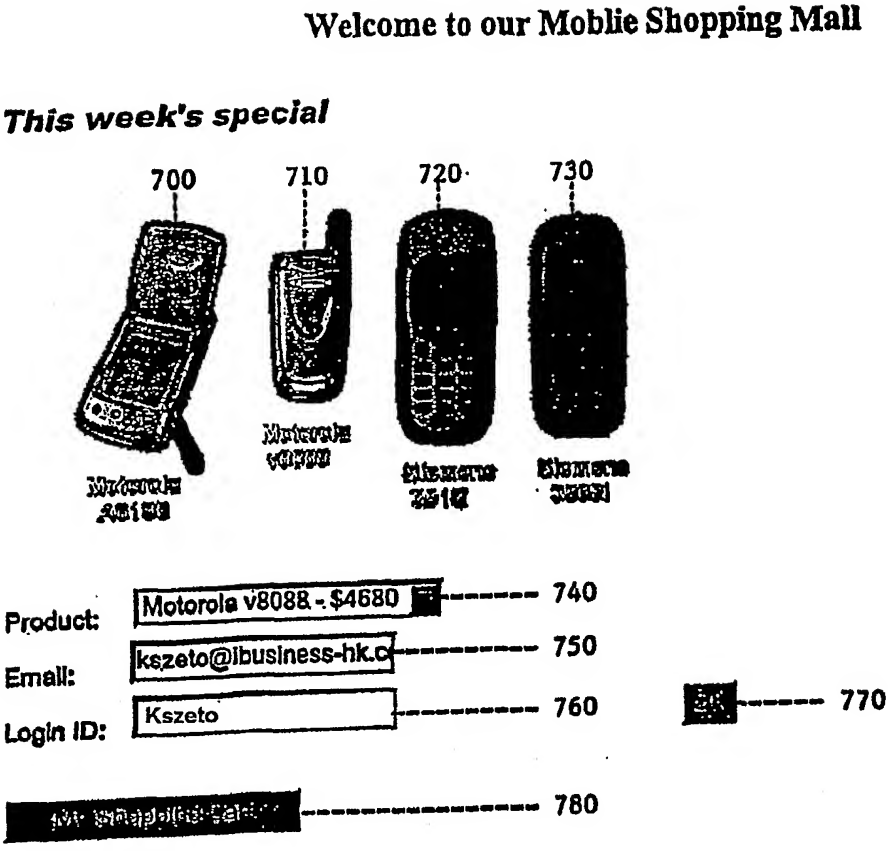

Welcome to our Moblie Shopping Mall
This week's special
700
710
720
730
Product:
Motorola v8088 - $4680
740
Email:
kszeto@ibusiness-hk.c
750
Login ID:
Kszeto
760
770
780

FIG . 8

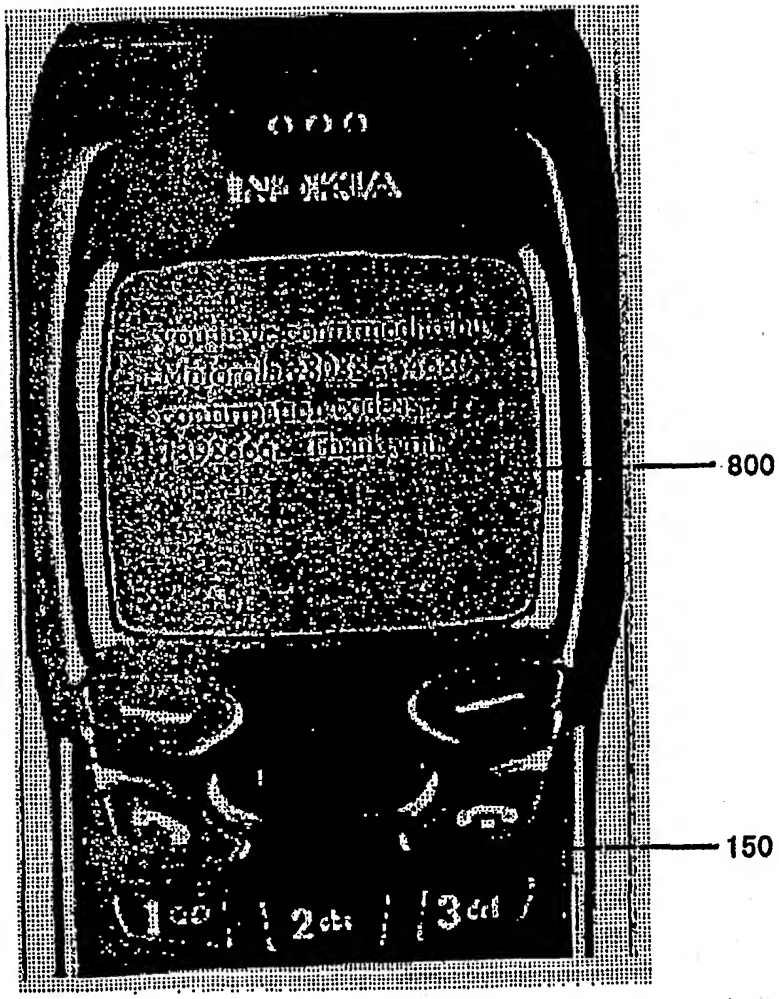


FIG .9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN00/00364

A. CLASSIFICATION OF SUBJECT MATTER

G06F15/00 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7 G06F15/00 H04Q7/38 H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP-A-2000029832 (HITACHI LTD)28.Jan 2000(28.01.00) 全文	1-57
A	US-A-5966662 (NOKIA TELECOM OY)12.Oct 1999(12.10.99) 全文	1-57

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12.Mar 2001(12.03.01)	29 MAR 2001
Name and mailing address of the ISA/CN 6 Xitucheng Rd., Jimen Bridge, Haidian District, 100088 Beijing, China Facsimile No. 86-10-62019451	Authorized officer Wang Tao Telephone No. 86-10-62093049

Form PCT/ISA /210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN00/00364

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP-A-2000029832	28.01.00	None	
US-A-5966662	12.10.99	WO-A-9601030	11.01.96
		AU-A-2793895	25.01.96
		FI-A-9403104	29.12.95
		EP-A-0768011	16.04.97
		JP-T-10502229	24.02.98